AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Northern District of California

United States of America
v.
MARK DJANGO HICKS JR.,a/k/a Amir Rashad,
SUSAN ARREOLA-MARTIN,
CHRISTOPHER TODD POOL,
TYRONE ALEXANDER JONES

Defendant(s)

Case No. 3 20 70160

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of October 2018 to Present in the county of Contra Costa in the Northern District of California, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. 1349	Conspiracy to Commit Wire Fraud

UNDER SEAL

This criminal complaint is based on these facts:

See Attached Affidavit of FBI Special Agent Armando Delgado-Campos

☐ Continued on the attached sheet.

Approved as to form
AUSA David Ward

Complainant's signature

FBI Special Agent Armando Delgado-Campos
Printed name and title

Sworn to before me and signed in my presence.

Date: 2/11/2020

Judge's signature

City and state: San Francisco, California

Hon. Chief Magistrate Judge Joseph C. Spero
Printed name and title

AFFIDAVIT IN SUPPORT OF APPLICATIONS FOR SEARCH WARRANTS, ARREST WARRANTS, AND A CRIMINAL COMPLAINT

I, Armando Delgado-Campos, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I submit this affidavit in support of search warrants, as further described herein and in Attachments A-1, A-2 and A-3, for the following premises:

- **Target Location #1**: 4865 Mallard Court, Oakley, CA 94561:
- **Target Location #2:** 2910 Humphrey Avenue, Richmond, CA 94804;
- **Vehicle #1:** 2007 Black Cadillac Escalade, VIN 1GYFK63857R289840, California License Plate (CALP) 5XFE387;
- **Vehicle #2**: 2015 Mercedes Benz, S550 model, VIN number WDDUG8CB4FA149769, CALP 8CVR018;
- **Vehicle #3:** 2012 Nissan sedan, VIN number 3N1CN7AP5CL836478, CALP 6TXM823;

2. I am a Special Agent of the Federal Bureau of Investigation ("FBI") and have been so employed since 2005. For the past fourteen years, I have been assigned to the San Francisco Division of the FBI where I have been responsible for investigating complex financial crimes. During my career with the FBI, I have received specialized training in the investigation of financial and computer-related crimes. In addition, I have participated in numerous criminal investigations involving wire fraud, mail fraud, bank fraud, and money laundering. In those matters, I have submitted probable cause statements in the form of sworn affidavits to federal magistrate judges in the Northern and Eastern Districts of California. I have also participated in the execution of various arrests and search warrants in which business and personal documents, bank records, computers, telephones and other evidence of federal crimes, including fraud offenses, have been seized.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested

warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that a violation of 18 U.S.C. § 1349 (conspiracy to commit wire fraud) (the "**Target Offense**") has been committed and is continuing to be committed by Amir Malik Sharif Rashad, aka Mark Django Hicks, aka "Kafani" (HICKS), Tyrone Alexander Jones (JONES), Susan Arreola-Martin (ARREOLA-MARTIN), Christopher Todd Pool (POOL), and other co-conspirators, and that evidence of these crimes, as further described in Attachment B, will be located at the residences of HICKS (**Target Location #1),** JONES **(Target Location #2),** and in **Vehicles #1, #2, #3,** as further described in ¶¶ 84-87 and Attachments A-1 and A-2.

FACTS ESTABLISHING PROBABLE CAUSE

I. Introduction

5. Since July 2019, the FBI has been investigating a mortgage loan fraud conspiracy targeting individuals in the San Francisco Bay and Los Angeles areas. The investigation was started from a referral received from the Alameda County District Attorney's Office (ACDAO), and now also involves the U.S. Secret Service, and the Los Angeles County District Attorney's Office. In each of the instances being investigated, an unknown subject or subjects stole personal identifying information from the victim, used that information to open a bank account in the victim's name, and established an email account using the victim's name. The subjects would then use the victim's identity to obtain a refinance loan, using the victim's property as collateral. Some of the loans were approved and the money was released. Other loans were cancelled prior to the release of some or all of the money.

6. For the approved loans, the subjects directed the loan proceeds to the bank accounts opened in the victim's names. At all times, the subjects maintained control and access of the bank accounts, including full access to the "online banking" area of the accounts. After the accounts received the money, the funds were extracted via ATM cash withdrawals, store debits to pay for the purchase of high-end goods, and wire-transfers to other bank accounts

controlled and opened by the subjects. Additionally, the suspects would make wire transfers to gold and other precious metals dealers to buy tens or hundreds of thousands of dollars in precious metals, primarily gold or silver coins and bars.

7. In each instance and for each victim, the subjects created a Google email account with an associated Google Voice telephone number and sometimes used prepaid telephone numbers. The email accounts were created with a variation of the victims' names. The email accounts, Google Voice telephone numbers, and prepaid telephone numbers were used to maintain contact with the banks, title companies, gold dealers, and others.

8. The evidence developed to date points to HICKS as the ringleader of this scheme. HICKS, 40, is an Oakland rapper and musician with an extensive criminal record dating to 1995, including convictions for robbery, grand theft, illegal use of credit cards, and felon in possession. In May 2015, HICKS pleaded guilty to a federal indictment filed in the Northern District of California charging him with Conspiracy to Commit Mail and Wire Fraud, 18 U.S.C. § 1349, and Bank Fraud, 18 U.S.C. § 1344 (1) & (2). HICKS was sentenced to 39 months in jail, five years of supervised release, and $258,400 in restitution. HICKS was released from federal custody in November 2017, and is currently under federal supervision.

9. On September 28, 2013, HICKS was shot five times after shooting a rap video in East Oakland. He was paralyzed from the waist down and is in a wheelchair.

II. Mortgage Loan Fraud Against Victim #1 (DAT)

A. HICKS Is Tied to Loans in Victim #1's Name

10. Victim #1 (DAT) is the owner of two properties in Oakland, CA, located next to each other. Both properties are on the same block as HICKS' mother's residence.

11. On March 20, 2019, Victim #1 contacted the ACDAO and reported that she believed she had been the victim of loan fraud. Victim #1, along with her trust attorney, were interviewed by the ACDAO. Victim #1 was again interviewed in June 2019 by the ACDAO and the FBI. I was present for that interview.

12. Victim #1 said that in 2010, she placed her two properties in a trust administered by JL, a real estate attorney in San Francisco. In 2017, JL passed away and left his law practice to another real estate attorney (Victim #1's Attorney) also based in San Francisco. One of the cases Victim #1's Attorney inherited was Victim #1's trust.

13. On March 1, 2019, Victim #1 received an unexpected bill for $360 from Victim #1's Attorney for services rendered in connection with a "loan letter" she prepared. Victim #1 had not asked Victim #1's Attorney to prepare any "loan letters." Victim #1 immediately contacted Victim #1's Attorney, and they determined Victim #1 was a victim of identity theft and fraud.

14. According to Victim #1's Attorney, in late October 2018, unbeknownst to Victim #1, an individual who identified himself as Victim #1's son contacted Victim #1's Attorney by email and from telephone number 510-990-0428 to request a copy of his mother's trust. The attorney complied and gave him a copy of Victim #1's trust.

15. Based on my investigation, including a review of text messages obtained via a search warrant for the Google account tied to this number (see ¶¶ 34-37) I have determined that phone number 510-990-0428 (hereinafter "HICKS Phone #1") was used by HICKS to perpetrate the fraud against Victim #1.

16. In December 2018, the individual claiming to be the victim's son again contacted Victim #1's Attorney by email and said that his mother was trying to get a refinance loan. As part of the approval process, the "son" said the loan broker needed a letter from the attorney's office stating that his mother was capable of handling her financial affairs and understood the loan was a "high cost loan." The number he provided was HICKS Phone #1, and said he could be reached at that number.

17. On December 11, 2018, Victim #1's attorney sent an email to the victim's son with the requested letter.

18. On November 9, 2018, two bank accounts were opened at BofA in Victim #1's

name. I have obtained and reviewed the account application and bank statements for these accounts. The documents used to open the accounts, accounts which Victim #1 has confirmed she did not create or authorize, included Victim #1's actual Social Security number, date of birth, and a mailing address in Richmond, CA. Gold purchases with proceeds of this and other frauds being perpetrated by HICKS and others were sent to the Richmond address. On February 2019, the mailing address on both of the BofA accounts in Victim #1's name was changed to an address in Vallejo, CA., where multiple shipments of gold coins and bars purchased with proceeds from this fraud conspiracy have been shipped (hereinafter "Gold Delivery Residence").

19. In December 2018, a $300,000 mortgage loan was taken out through North Coast Financial, with one of Victim #1's properties in Oakland as collateral. In March 2019, a second loan was taken out, also through North Coast Financial, for $250,000, using Victim #1's second residence in Oakland as collateral. On the corresponding loan application used for both loans, the applicant's name was listed as Victim #1, which HICKS Phone #1 as the phone number, with the same Richmond address. Once the loans closed, the loan proceeds were wire-transferred to the BoA checking account in the name of Victim #1.

B. ARREOLA-MARTIN Impersonates Victim #1 to Notarize Fraudulent Loan Documents

20. On December 13, 2018, a notary public (Notary 1), was contacted by a mobile notary service and asked to contact Victim #1 to schedule a document notarization. The email included Hick's Phone #1. An investigator from the ACDAO has interviewed Notary 1, who stated that the first time Notary 1 called this number, it was answered by a female; on the second occasion it was answered by a male. On December 13, 2018, Notary 1 telephoned HICKS' Phone #1, and the number was answered by a male, who said he was driving his mother Victim #1 to meet with Notary 1. Later that day, Notary 1 met with the woman claiming to be Victim #1, and notarized loan documents for her. Notary 1 stated that she obtained two fingerprints from the individual claiming to be Victim #1 for the notary journal, and took a photograph of

Victim #1's California Driver's License (CDL). I have examined that CDL, and identified the woman in the picture as ARREOLA-MARTIN. The fingerprints from the notary book were submitted to the Alameda County Sheriff's Department, Criminal Identification Bureau, and identification is pending.

21. On March 8, 2019, a second notary (Notary 2), met with a woman claiming to be Victim #1 to notarize documents related to the second North Coast Financial loan. Notary 2's husband (husband), went with her. Notary 2 and her husband were interviewed in June 2019. They stated that they both met with the woman identifying herself as Victim #1, and at the time, Notary 2 said she was suspicious that Victim #1's CDL was fake. But her husband told her not to worry about it, and they notarized the loan documents. Notary 2 and her husband were separately shown double blind photo lineups, and both identified ARREOLA-MARTIN as the individual who signed the notary documents and showed them the CDL in Victim #1's The thumbprint from Notary 2's notary journal was submitted to the Alameda County Sheriff's Department, Criminal Identification Bureau, but they were unable to match the print to an individual.

C. HICKS Brother and HICKS Brother's Girlfriend Both Live at Target Location #2 and Made ATM Withdrawals of $31,800 From Victim #1 BofA Account

22. Between December 19, 2018 and February 27, 2019, $33,200 was withdrawn from the Victim #1 fraudulently opened checking account at BofA in ATM withdrawals. Between December 19, 2018 and March 13, 2019, five outgoing wire transfers were made. Four of the wire transfers, totaling $78,686.76, were sent to APMEX, a gold coin dealer in Oklahoma, and one, for $144,000, was sent to another gold dealer, Goldline, Inc., based in Los Angeles, CA.

23. In February 2019 alone, $31,800 was withdrawn from the Victim #1 fraudulently opened checking account at BofA in ATM transactions at BofA branches in Antioch, CA, Pittsburg, CA, and Richmond, CA. I have obtained and reviewed ATM surveillance videos of several of these transactions, and identified HICKS' brother as the individual withdrawing

money in at least one of the transactions. In a separate transaction, I was able to identify an individual I believe is HICKS' brother's girlfriend and roommate as the individual withdrawing funds from the Victim #1 account.

24. The girlfriend, according to the California Department of Motor Vehicles, appears as a former owner of a 1996 Chevrolet vehicle with expired tags, registered at **Target Location #2.** According to Lexis Nexis, the girlfriend's most current address is **Target Location #2.** Records obtained from the California Department of Corrections show that the girlfriend was listed as a friend and known associate of HICKS' brother.

D. HICKS Linked to IP Address From Victim #1 Bank Account

25. I obtained Internet Protocol (IP) addresses from BofA for all the logins to the online banking area of the accounts opened in the name of Victim #1. I identified two logins, on December 19, 2018, and February 21, 2019 from IP addresses 73.223.0.119 and 76.102.173.107, respectively. I requested subscriber records from Comcast for both IP addresses and was informed that the subscriber of IP address 73.223.0.119 could not be located. However, Comcast identified the subscriber of IP address 76.102.173.107 as AB, with a service address in Antioch, CA, that I had identified as being HICKS' residence at the time. I know this was HICKS' residence from US Probation records, and from physical surveillance of the Antioch address, during which I saw two vehicles registered to HICKS' mother. These vehicles were a 2007 Cadillac Escalade parked in the driveway and a 2012 Nissan Sentra parked on the curb. I also saw a 2005 Acura sedan, parked in the driveway, registered to AB, HICKS' girlfriend. In addition, this address was provided as HICKS' in an anonymous tip to the FBI. (See ¶¶ 46-47).

26. I have learned from my investigation that AB, the Comcast subscriber for the Antioch address appears to be HICKS' current girlfriend and caretaker.

27. The BofA account included phone number 510-697-6813. I obtained subscriber records for telephone number 510-697-6813 from AT&T. It is an active account in the name of HICKS' mother. The mailing address associated with the telephone number 510-697-6813 is the

address of HICKS' mother in Oakland. This residence is on the same block as both of Victim #1's residences which were used as collateral to obtain fraudulent loans in Victim #1's name.

28. The IP address 73.223.0.119 (the one that Comcast could not identify) I have determined was used to access the online bank accounts of two other BofA accounts opened in the names of Victim #6 and Victim #5, two other individuals who were victims of this mortgage loan fraud scheme. In addition, IP address 73.223.0.119 was used to apply for an American Express credit card in the name of Victim #6.

E. HICKS is Identified as Individual Placing Gold Coin Orders as Victim #1

29. Between December 19, 2018 and March 13, 2019 five outgoing wire transfers were made from the bank account in Victim #1's name. Four of the wire transfers, totaling $78,686.76, were sent to APMEX, a gold coin dealer in Oklahoma, and one, for $144,000, was sent to another gold dealer, Goldline, Inc., based in Los Angeles, CA.

30. I obtained records from APMEX and determined that an individual claiming to be Victim #1, using an email created in her name and calling from HICKS' Phone #1 purchased approximately 60 gold coins described as "Gold American Eagle" and "Gold Buffalo." The coins were shipped in four separate packages delivered in or around February 27, 28, March 5 and March 13, 2019. All the coins were shipped to the Gold Delivery Residence in Vallejo.

31. I also obtained from APMEX three audio recordings of telephone calls made from HICKS' Phone #1 by a person claiming to be Victim #1, attempting to conceal and change his voice. I have listened to these calls and believe that they are HICKS, whose voice I recognize from watching public videos he posted on his public Instagram profile.

32. On December 24, 2019, I obtained records from Goldline regarding a wire transfer for $144,000 received from the same BofA account in the name of Victim #1. Goldline stated that they received the money on December 17, 2018, as payment for "100 x 1oz Gold Eagles" coins that were delivered to the same address in Richmond listed on the bank account Victim #1's name. The order was placed in the name of Victim #1.

33. I have obtained recordings of calls from Goldline from a person identifying themselves as Victim #, and I recognize the voice as being HICKS.

34. Further, I played two calls to Goldline from a person claiming to be Victim #1 (on December 17 and December 20, 2018) for HICKS' probation officer. She recognized his voice from the December 17 call, and said it appeared he was trying to change his voice. She said that the call on December 20 sounded like HICKS, but she couldn't say definitively.

F. Text Messages, Emails, and HICKS' Instagram Account Link HICKS to Loan Fraud Conspiracy

35. I have obtained account information, location data, and text message exchanges from Google Inc. for HICKS Phone #1. On November 17, 2018, HICKS Phone #1 sent a text message that said "we good I just need a granny." Based on the timing of this conversation, I believe HICKS here is referring to the need for an older woman to impersonate Victim #1, who is an elderly woman. In fact, less than a month later, on December 13, 2018, ARREOLA-MARTIN, age 69, impersonated Victim #1 to notarize documents.

36. On March 14, 2019, there is the following exchange of text messages between HICKS Phone #1 and a telephone number with a 213 area code.

213: "*Nigga that's fucked up that I didn't get my chop off that 142k that was in the account. No matter what the situation ole girl signed for that shit.*"

HICKS Phone #1: "*Wtf it's a block.*"

213: "*Naw nigga I'm talking about all that Neiman Marcus and all that shit after I heard it was blocked*"

213: "*I want my chop off that 142 that was in there.*"

213: "*All that shopping Smurf was doing came out that 142.*"

HICKS Phone #1: "*Bra I deal with my bro.*"

37. Based on our investigation, I know that HICKS' brother is referred to and known as "Smurf." I also know that someone using funds from the BofA account in Victim #1's name

made approximately $74,000 in purchases from different stores in the San Francisco Bay Area, including Neiman Marcus, Macy's, Best Buy, Nordstrom, Sunglass Hut, Target, Barney's, Ugg and Guitar Center. The purchases were made from approximately February 19 to February 28, 2019, two weeks before the above-described text message exchange.

38. The text messages I reviewed, sent from and received by HICKS' Phone #1 do not clearly show the identity of the persons involved in the conversations. However, on April 9, 2019, in response to a question asked in an incoming text message, "*what's the Avid account login? Just the email*," HICKS Phone #1 replied with "*icekingmusic01@gmail.com*."

39. The Twitter profile for "@kafani" lists bayonaire.kafani@gmail.com as a contact for HICKS. The location icon associated with this profile shows "ICE KING OAKLAND."

40. The Instagram profile for "@kafani" shows the same individual as the Twitter profile and lists the email bayonaire.kafani@gmail.com way to contact the account owner.

41. On December 23, 2019, I obtained a search warrant for email account: bayonaire.kafani@gmail.com. In my review of those emails, I identified two incoming emails, sent on May 1 and May 2, 2019, from icekingmusic01@gmail.com to bayonaire.kafani@gmail.com.

42. Open source internet searches identified public Twitter and Instagram profiles that include several pictures and videos that match HICKS' driver's license photo, and use the moniker "Kafani," which I know is an a/k/a for HICKS.

43. On January 26, 2020, I searched the internet for "Avid login" and found a webpage, www.avid.com, a company specializing in audio and video multimedia equipment and software. I know from this case that HICKS is a local rap musician, and that he produces videos and songs, therefore using equipment and software such as the one distributed and sold by Avid.

44. The Oakland Police Department, Intelligence Unit, provided investigators working with me on this case with information that HICKS grew up and is associated with an Oakland street gang named, "Ice City;" hence, HICKS fondness of using the term, "ice."

45. For example, a review of the public posts in the Instagram profile for "@kafani" shows a picture posted on October 27, 2019 of another Instagram user identified as "smurfhicks." On the post, "@kafani" included a message that reads "Everybody wish my brother @smurhicks Happy Birthday…It's a real nigga Holiday "#alwaystalkinmoney #ATM #Icekingmusic." I believe the individual in this picture is HICKS' brother.

G. Complaint to the FBI Alleges HICKS Involved in Wire Fraud; Names Two Specific Victims

46. On April 25, 2019, the FBI received a complaint through the internet from an individual who identified himself as Victim #5. The complaint identified "MARK HICKS aka AMIR RASHAD," as the individual responsible of doing "wire fraud" in the amount of $50,000 against Victim #5. The complainant added that HICKS "tried wiring money from an account under the name of another victim, JD (Victim #7), and he is still out committing crimes and putting other people in danger." The complaint stated that HICKS had prior federal convictions and was on federal probation. In fact, HICKS is currently on supervised release following a 2015 conviction for Bank Fraud and Conspiracy to Commit Mail and Wire Fraud, for which he was sentenced to 39 months in prison.

47. The complainant identified the Antioch, CA address noted above as HICKS' current residence and HICKS mother's address in Oakland, claiming that HICKS also uses that address. In my investigation, I have learned that until Mid-December 2019 HICKS lived at the Antioch address, and that HICKS' mother lives at the address in Oakland provided by the complainant. I have also learned that sometime in mid-December 2019 HICKS moved to **Target Location #1.**

48. We are currently investigating reports from Victims #5 and #7 that someone obtained their personal identifying information without permission, and attempted to obtain hundreds of thousands of dollars in fraudulent loans using their properties as collateral (See Sec. V below).

III. HICKS and JONES Commit Mortgage Loan Fraud Against DB (Victim #2)

49. Around December 2019, the identity of Los Angeles resident DB ("Victim #2), was stolen and used to obtain a $1 million loan against Victim #2's property, located in Beverly Hills, CA. The corresponding loan documents were notarized at an address in Fairfield, CA and signed by an individual who used a California Driver's License, number D9765656, in the name of Victim #2. The Los Angeles County District Attorney's Office ("LACDA") was made aware of this fraudulent transaction and opened an investigation, and I was alerted to their matter on January 17, 2020. At that time, I determined that their investigation involved some of the same suspects and the same pattern as the HICKS investigation.

50. As part of their investigation into the Victim #2 fraud, the LACDA obtained and analyzed fingerprints from the notary book signed by the individual purporting to be Victim #2. They determined that the identity of that individual was JONES.

51. I have reviewed the image on the CDL used for the fraudulent notarization on the Victim #2 loan documents, and based on my comparison of the photo to JONES' legitimate CDL photo, I have determined they are the same individual. On January 30, 2020, I queried California Department of Motor Vehicle's driver's license records for CDLN number D9765656 and determined that the number belongs to another individual with no apparent relation to Victim #2 or JONES.

A. HICKS Orders Gold Coins and Bars by Phone Posing as Victim #2

52. As part of our investigation, we learned that U.S. Gold Bureau, a gold dealer in Austin, TX, had information on a recent purchase of gold coins and bars made by an individual identifying himself as Victim #2. I contacted U.S. Gold Bureau and confirmed that on December 2, 6, and 12, 2019, they received payment for three orders for gold coins and bars, totaling $939,999.97, from a person who identified himself as Victim #2. All three orders were shipped to the Gold Delivery Residence in Vallejo.

53. U.S. Gold Bureau told the FBI that the person calling to place these orders had called from two telephone numbers, one of them being 510-332-3732 (HICKS Phone #2), which

as described more fully below, we believe is the phone HICKS used for the Victim #2 fraud. U.S. Gold Bureau also provided dates and times of the calls, as well as recordings.

B. Calls to U.S. Gold Bureau Came From Vicinity of HICKS' Residence

54. On February 1, pursuant to a federal search warrant signed by the Honorable Sallie Kim, I obtained historical cell tower location data from AT&T for HICKS Phone #2. An FBI Cellular Analysis Survey Team (CAST) special agent has been analyzing that data, and we have determined that multiple calls from HICKS Phone #2 to the U.S. Gold Bureau occurred when the phone was in the vicinity of **Target Location #1**, HICKS' current residence.

a. On January 16, 2020 at 12:47 pm PT, U.S. Gold Bureau recorded an 8 minute, 13 second call with an individual speaking from HICKS Phone #2 discussing the Victim #2 gold purchase. According to the FBI CAST agent, at the time, that number was connecting to one of the two cell towers closest to HICKS' residence, and call records show a call of the same duration at the same time.

b. On January 22, 2020 at 7:44 am PT, U.S. Gold Bureau recorded a 5 minute, 45 second call with an individual calling from HICKS Phone #2 inquiring about the Victim #2 gold purchase. At the time, that number was connecting to one of the two cell towers closest to HICKS' residence, and call records show a call of the same duration at the same time.

c. On January 24, 2020 at 9:08 am PT, U.S. Gold Bureau recorded a 2 minute, 19 second call with an individual calling from HICKS Phone #2 inquiring about the Victim #2 gold purchase. According to the FBI CAST agent, at the time, that number was connecting to one of the two cell towers closest to HICKS' residence, and call records show a call of the same duration at the same time.

d. In addition to these calls, CAST analysis of the toll records for HICKS Phone #2 show six other calls to the U.S. Gold Bureau's number in Austin, all of

which were made in December 2019 from the cell tower in the vicinity of the Antioch address, which I know to have been HICKS' residence at that time.

C. HICKS' Voice Identified on Gold Bureau Calls Posing as Victim #2

55. I listened to the recorded calls from HICKS Phone #2 provided by the U.S. Gold Bureau and recognized that the individual calling and identifying himself as Victim #2 was in fact HICKS. This voice also matches the voice of an individual who ordered gold coins from other gold dealers in transactions we had identified as part of this investigation.

56. I have also reviewed several videos that have been published on HICKS' public Instagram page and the way HICKS speaks in his Instagram posts matches the voice on the recorded calls to the gold dealers and the title company.

57. I have also played the recordings to another FBI Agent on my squad who is familiar with HICKS' voice from a prior investigation, and he also identified the voice on the recordings as that of HICKS.

58. And as noted above, on February 7, 2020, a U.S. Secret Service agent involved in this investigation played two recordings of HICKS speaking to the U.S. Gold Bureau and identifying himself as Victim #2, on December 2, 2019, and January 29, 2020, for HICKS' probation officer, and she recognized the voice on the both recordings as HICKS.

59. On January 22, 2020, U.S. Gold Bureau received a bank wire for $24,000, purporting to come from Victim #2, for the purchase of additional gold bars. The individual called U.S. Gold Bureau from HICKS Phone #2 and, based on the sound of his voice, it is believed he is the subject of this investigation, HICKS, and the same individual previously identified for the orders totaling $939,999.97. The order on January 22, 2020, was for 13 one ounce gold bars, to be shipped to the Gold Delivery Residence in Vallejo, the same location where the December orders totaling $939,999.97 had been delivered.

D. JONES is Involved in Controlled Delivery to Gold Delivery Residence in Vallejo

60. On January 28, 2020, the FBI conducted a controlled delivery of the order paid for on January 22, 2020 for $24,000. However, at the direction of the FBI, instead of sending gold bars, U.S. Gold Bureau sent silver bars, worth only about $300. The shipment was sent through the U.S. Postal Service ("USPS") and the delivery was video and audio recorded.

61. The FBI set up surveillance around the exterior of the Gold Delivery Residence in Vallejo, California before and after the package was delivered. Prior to the delivery, a car registered to HICKS' brother and being driven by a black male, was seen dropping off JONES at the Gold Delivery residence. Later that day, we observed the same vehicle arriving at **Target Location #2**, the residence of HICKS' brother.

62. I have reviewed the corresponding video, and identified the person who received the package as JONES. JONES was sitting outside the Gold Delivery Residence when the delivery was made. JONES identified himself as "David," said he lived at the Gold Delivery Residence, and signed his name as Victim #2 on the corresponding USPS form. No ID was requested, so he did not produce identification.

63. After the package was delivered, JONES was seen departing from the Gold Delivery Residence and immediately taking the package to **Target Location #2,** where he met with several other individuals. One of the individuals who was seen at this residence is believed to be HICKS' brother. HICKS' brother is a registered sex offender, and according to the Megan's Law website, he resides at **Target Location #2**

64. On January 29, 2020, U.S. Gold Bureau was contacted from telephone number 702-200-8932 by an individual identifying himself as Victim #2. "Victim #2" claimed he had lost the phone with number HICKS Phone #2 and had a new telephone number. "Victim #2" complained that he had ordered gold bars but instead had received silver bars. A call service representative of U.S. Gold Bureau told the individual that it was a mistake made by the shipping department and that his order would be fulfilled as soon the silver bars were returned to U.S.

Gold Bureau. U.S. Gold Bureau agreed to send a prepaid envelope or prepaid label to facilitate the shipping of the silver bars back to US Gold Bureau.

65. On February 6, 2020, the silver bars were returned to U.S. Gold Bureau. U.S. Gold Bureau, at the FBI's instruction, will tell HICKS that the bars and coins will be shipped on Monday, February 10, to arrive at the Gold Delivery Residence on Wednesday, February 12.

IV. Mortgage Loan Fraud, Identify Theft Against Victims #3 and #4 (LM & BM)

66. On October 14, 2019, Victim #3 (LM) contacted the Orinda Police Department regarding an unauthorized loan attained using her identity and that of her husband, Victim #4 (BM). The $325,000 unauthorized loan was against Victims #3 and #4"s property located in Orinda, CA. Loan documents provided by Placer Title Company show that the fraudulently obtain funds were to be wired to CIT Bank, Account # *****1209.

67. The Contra Costa County District Attorney's Office investigated and, on October 24, 2019, executed a search warrant for documents and records related to CIT Bank Account # ******1209. The results of the search warrant and review of bank records indicate that Account # *****1209 was opened using the identities of Victims #3 and #4. Associated with this account are telephone numbers 650-229-8705 and 510-697-4553 as well as Gmail email addresses using the names of Victims #3 and #4. USSS Special Agent Stephen Miller has spoken with Victims #3 and #4, and both confirmed that they did not open CIT Bank Account #******1209, nor did they create the Gmail email accounts in their name.

A. HICKS Opens CIT Bank Account in Victims #3 and #4's Name

68. On December 16, 2019, CIT Bank provided USSS SA Miller with bank records associated with Account # *****1209. Included in the records are recorded telephone calls that originated from telephone number 650-229-8705, the number that appears on the Placer Title loan documents and also provided to CIT Bank when Account # ******1209 was opened. SA Miller reviewed these recorded telephone calls and heard the caller's voice provide the email in the name of Victim #4 to the CIT Bank employee so that a verification code could be sent to the

email address. On the recordings, the subject's voice is heard providing the CIT Bank employee with correct verification codes sent to the email in Victim #4's name.

69. I have obtained and listened to recorded telephone conversations with the individual who open CIT Bank Account # ******1209, and I recognized the voice as matching that of HICKS, the same voice that made calls to U.S. Gold Bureau, Goldline, and APMEX tied to the frauds targeting Victims #1 and Victim #2.

B. HICKS Voice is Identified as the Caller Impersonating Victim #4.

70. On October 3, 2019, an individual identifying himself as Victim #4, telephoned U.S. Gold Bureau to order gold coins and bars. One of the agents on this case played this recording to HICKS' probation officer, who said that she recognized the voice on the recording as being HICKS.

C. ARREOLA-MARTIN and POOL Impersonate Victims #3 and #4

71. On September 11, 15, and 30, 2019, individuals identifying themselves as Victims #3 and #4 met with Notary 3 at the Starbucks in El Cerrito, CA to sign and notarize documents related to the loan against Victim #3 and #4's property in Orinda, CA. An Orinda Police Department Detective has interviewed Notary 3, and obtained her notary records.

72. On November 12, 2019, Contra Costa County District Attorney (CCCDA) Senior Inspector Richard Van Koll and Inspector Steven Cheatham met Notary 3 to conduct a photo-lineup. Notary 3 was shown a photo lineup of individuals, and identified a picture of ARREOLA-MARTIN as the individual identifying herself as Victim #3.

73. On November 15, 2019, CCCDA Senior Inspector Van Koll and Inspector Cheatham met again with Notary 3. Notary 3 was shown a photo lineup of individuals, and identified a picture of POOL as the individual who claimed to be Victim #4.

74. The Contra Costa Sheriff's Crime Lab had the fingerprints given to the notary analyzed, and the fingerprint of the individual identifying himself as Victim #4 was that of POOL, and the fingerprint of the individual identifying himself as Victim #3 was that of

ARREOLA-MARTIN.

V. Mortgage Loan Fraud, Identify Theft from (DR & CR) Victims #5 and #6

75. On May 6, 2019, Victim #5 (DR) was interviewed in response to the April 25, 2019 anonymous complaint sent to the FBI in his name. Victim #5 stated that he did not file a complaint with the FBI. However, he did state that in October 2018, someone tried to obtain a cash-out loan against his business property in Redwood City, CA.

76. In November 2019, a loan officer from Coast to Coast Lending in San Juan Capistrano, CA, was interviewed by the FBI. The loan officer stated that in early October 2018, he received a loan application in the name of Victim #5 and his wife CR (Victim #6) for a cash-out refinancing loan against their property, in Redwood City, CA. While the loan was being processed, an individual identifying himself as Victim #5 used an email in Victim #5's name and telephone number 650-216-8778 to communicate with the loan officer. The loan closed successfully. As a result, on October 12, 2018, the loan proceeds, totaling $470.609.35, were wire-transferred to a BofA account in the name of "Victim #5 Enterprises," number ******9229. A few days after closing the loan, the loan officer was informed that Victim #5's bank account, used to receive the loan funds, was frozen due to fraud. The loan officer also learned that the loan signing was not done at Victim #5 and #6s residence, as was instructed, but instead at a Starbucks in Stockton, CA. By the time the funds were frozen approximately $94,000 had been withdrawn from the account.

A. HICKS Purchases Gold Using Funds from Victims #5, #6 Loan

77. Of this amount, $73,442 was wired to Goldline Inc. to purchase gold bars and coins. The calls to Goldline were recorded, and the individual is the same voice I recognize as HICKS, and the same voice that was recorded in calls to U.S. Gold Bureau, APMEX, and CIT Bank as part of the fraud against Victim #1, Victim #2, and Victims #5, and #6.

78. Separately, I played an October 15, 2018 call to Goldline from an individual purporting to be Victim #5 for HICKS' probation officer. She stated that it was possibly HICKS,

and that the rasp in the voice was similar to his.

B. ARREOLA-MARTIN and Co-Conspirator Impersonate Victims #5 and #6 to Notarize Fraudulent Loan Documents

79. On October 10, 2018 Notary 4 was contacted and asked to meet Victims #5 and #6 to notarize loan documents. Later that day, Notary 4 met with two individuals claiming to be Victims #5 and #6. Both individuals provided a fingerprint in the notary book, and produced California Driver's Licenses in the names of Victims #5 and #6. Victim #5 used California Driver's License number C***3177 and Victim #6 used California Driver's License number D***0032. Both California Driver's Licenses had the same residence address listed as 411 El Dorado Street, Vallejo, CA 94590.

80. I have obtained records from the California Department of Motor Vehicles for both driver's license numbers and determined they do not belong to anybody with the last name of Victims #5 and #6. In fact, the driver's license number used by the purported Victim #5 belongs to a deceased individual. The other number used by the purported Victim #6 is assigned to a person with a residence in Chino, CA. However, the image on Victim #5's CDL matches that of ARREOLA-MARTIN. The fingerprints from the notary book are being analyzed by the Alameda County Central Identification Bureau.

81. On February 4, 2020, I met with Notary 4, the notary who met with the individuals claiming to be Victims #5 and #6, and showed him a photo lineup of both ARREOLA-MARTIN and, separately, an unindicted co-conspirator. The notary said he was "85 percent" certain the woman identifying herself as Victim #6 was ARREOLA-MARTIN. The notary did not recognize the picture of the unindicted co-conspirator.

VI. Investigation of Target Locations

82. As part of my investigation, I have spoken with HICKS' federal probation officer, and she told me that HICKS is registered as living at **Target Location #1**. Further, on February 6, 2020, this probation officer visited HICKS at Target Location #1, and confirmed it is his current residence.

83. I have checked probation records for JONES, and confirmed that he currently lives at **Target Location #2.** The controlled delivery of silver bars and coins made by U.S. Gold Bureau in January 2020 were observed being taken by JONES to **Target Location #2**. HICKS brother, who was captured on ATM surveillance videos withdrawing funds form a BofA checking account set up in Victim #1's name, also lives at **Target Location #2**, as does his girlfriend, who was also captured on ATM surveillance videos withdrawing funds from the same Victim #1 BoA account.

84. FBI agents assigned to this investigation have observed **Vehicles #1** and **#3** at **Target Location #1** on multiple occasions, most recently on February 1, 2020. I was told by HICKS' probation officer that **Vehicle #2**, a 2015 Mercedes Benz S550 was kept in the garage at **Target Location #1**.

85. I have observed **Vehicle #3**, a Nissan Sentra, parked in front of **Target Location #1**, as well as in front of HICKS' former address in Antioch when he resided there. I have also observed what I believe is the same Nissan Sentra as the vehicle seen in an ATM surveillance video dropping off HICKS' brother's girlfriend to withdraw funds from Victim's #1 BofA account.

86. In a Facebook Live broadcast by HICKS that I have seen, HICKS can be heard bragging about having a "Mercedes 550" and the inside of what appears to be **Vehicle #2** is visible. Additionally, a 2015 Mercedes Benz S550 is registered to HICKS' mother, and to a foundation "The Take-A-Step Foundation" that is tied to HICKS.

87. **Vehicle #1**: I know from a previous investigation of HICKS that he is the owner of this vehicle, a Cadillac Escalade. The vehicle is currently registered to HICKS' mother's address in Oakland

VII. Types of Evidence to be Sought

88. Based on my training and experience, including experience investigating fraud schemes, there is probable cause to believe that certain electronic and paper documents and

evidence may be found in the target locations. For the bank accounts opened in the victims' names, there may be statements, checks, ATM cards, receipts, and other records. These can be in either paper or electronic form, and the possession of these types of documents is an indicator of the access and control over an account, and is therefore relevant to the conduct described above.

89. Based on my training and experience, I also believe that participants in fraud schemes as described above often communicate with other participants or with bank representatives, notaries, title companies, and gold dealers. As discussed above, there is evidence that HICKS communicated with co-conspirators, banks, title companies, and gold dealers. The presence of these communications at the subject location could constitute evidence of the crimes alleged.

90. Based on my experience in investigating fraud schemes such as described above, I have learned that the source of funds fraudulently obtained through loans using the victims' identities, as well as gold coins or bars, or other proceeds of the fraud, can be relevant evidence regarding the schemes because this type of evidence can show, among other things, the access and control of the relevant accounts, the participants in the scheme, and efforts to conceal the scheme. Also based on my training and experience, I know that financial records, in both paper and electronic form, are often retained for long periods of time and that in this case there is probable cause to believe that the target locations will contain records for relevant bank and other financial accounts.

VIII. Roles of Computers and Digital Devices in the Conspiracy

91. Based on my training and experience, I believe that computer equipment and/or electronic/digital devices (collectively, "digital devices") were used in furtherance of the above-described conspiracy, to wit: 1) to open bank accounts in the victims' names, 2) to contact title companies, loan brokers, and notaries, and 3) to contact gold sellers, and 4) to communicate with other conspirators, from digital devices using HICKS home IP address and from other locations.

I respectfully submit that there is probable cause to believe that the digital devices currently located at the target locations are the same equipment used to perpetrate this conspiracy.

92. Although the conduct that I am investigating occurred from at least 2018, I know based on my training and experience that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten.

93. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer use habits. This application seeks permission to search for and seize evidence of the crimes described above stored on digital devices, as well as any digital devices that constitute fruits and instrumentalities of the crimes. Searches of digital devices and seizure of any data will comport with the protocol set forth in Attachment C, which is hereby incorporated by reference.

94. Based upon my conversations with other law enforcement personnel and in my experience and training, I know that computers and other electronic equipment, including cell

phones and smart phones, are often used to facilitate and maintain records in complex financial crimes.

95. Based upon my training, experience, and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips. Some of these devices can be smaller than a thumbnail and can take several forms, including thumb drives, secure digital media used in phones and cameras, personal music devices, and similar items.

96. Based upon my training and experience, and information related to me by agents and others involved in the forensic examination of computers and digital devices, I know that computers and digital devices are often used to store information, very much the same way paper, ledgers, files and file cabinets are used to store information. I know that it is common today for businesses, including illegal ones, to utilize computers to conduct their business and to store information related thereto. I also know that it is common for individuals to have personal computers and to use these computers to conduct their personal affairs, their business affairs, and to store information related thereto.

97. Based upon my training and experience, and information related to me by agents and others involved in the forensic examination of computers and digital devices, I know that a forensic image is an exact physical copy of a data storage device. A forensic image captures all data on the subject media without viewing or changing the data in any way. Absent unusual circumstances, it is essential that a forensic image be obtained prior to conducting any search of data for information subject to seizure pursuant to the warrant. I also know that during the search of the premises it is not always possible to create a forensic image of or search digital devices or media for data. I also know that it is frequently necessary to remove digital devices or media for later laboratory evaluation off-site under controlled circumstances. This is true for a number of reasons, including the following:

98. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. Because there are so many different types of digital devices and software in use today, it is difficult to anticipate all of the necessary technical manuals, specialized equipment, and specific expertise necessary to conduct a thorough search of the media to ensure that the data will be preserved and evaluated in a useful manner.

99. Searching digital devices can require the use of precise, scientific procedures designed to maintain the integrity of the evidence. The recovery of such data may require the use of special software and procedures, such as those used in a law enforcement laboratory.

100. The volume of data stored on many digital devices is typically so large that it will be highly impractical to search for data during the execution of the physical search of the premises. Storage devices capable of storing 500 gigabytes of data are now common in desktop computers. It can take several hours, or even days, to image a single hard drive. The larger the drive, the longer it takes. Depending upon the number and size of the devices, the length of time that agents must remain onsite to image and examine digital devices can become impractical.

101. Because digital data may be vulnerable to inadvertent modification or destruction, a controlled environment, such as a law enforcement laboratory, may be essential to conduct a complete and accurate analysis of the digital devices from which the data will be extracted. Software used in a laboratory setting can often reveal the true nature of data. Moreover, a computer forensic reviewer needs a substantial amount of time to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband, or an instrumentality of a crime.

102. Analyzing the contents of a computer or other electronic storage device, even without significant technical difficulties, can be very challenging, and a variety of search and analytical methods must be used. For example, searching by keywords, which is a limited text-based search, often yields thousands of hits, each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a

relevant hit does not end the review process. The computer may have stored information about the data at issue which may not be searchable text, such as: who created it; when and how it was created, downloaded, or copied; when it was last accessed; when it was last modified; when it was last printed; and when it was deleted. The relevance of this kind of data is often contextual. Furthermore, many common e-mail, database, and spreadsheet applications do not store data as searchable text, thereby necessitating additional search procedures. To determine who created, modified, copied, downloaded, transferred, communicated about, deleted, or printed data requires a search of events that occurred on the computer in the time periods surrounding activity regarding the relevant data. Information about which users logged in, whether users shared passwords, whether a computer was connected to other computers or networks, and whether the users accessed or used other programs or services in the relevant time period, can help determine who was sitting at the keyboard.

103. Searching digital devices can require the use of precise, scientific procedures designed to recover latent data. The recovery of such data may require the use of special software and procedures. Data that represents electronic files or remnants of such files can be recovered months or even years after it has been downloaded onto a hard drive, deleted, or viewed via the Internet. Even when such files have been deleted, data can be recovered months or years later using readily available forensic tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in space on the hard drive or other storage media that is not allocated to an active file. In addition, a computer's operating system may keep a record of deleted data in a swap or recovery file or in a program specifically designed to restore the computer's settings in the event of a system failure.

104. This warrant seeks authority to seize contextual data, including evidence of how a digital device has been used, what it has been used for and who has used it. It can be very

important in criminal cases to seek "attribution" data so that an event or communication can be associated with a person. Based upon my training and experience, and information related to me by agents and others involved in the forensic examination of computers and digital devices, this authority is sought for a number of reasons:

a. In some instances, the computer "writes" to storage media without the specific knowledge or permission of the user. Generally, data or files that have been received via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to such data or files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve artifacts of electronic activity from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer usage. Logs of access to websites, file management/transfer programs, firewall permissions, and other data assist the examiner and investigators in creating a "picture" of what the computer was doing and how it was being used during the relevant time in question. Given the interrelationships of the data to various parts of the computer's operation, this information cannot be easily segregated.

b. Digital data on the hard drive that is not currently associated with any file may reveal evidence of a file that was once on the hard drive but has since been deleted or edited, or it could reveal a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, can

indicate the identity of the user of the digital device, or can point toward the existence of evidence in other locations (or on other devices).

c. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be learned from the absence of particular data on a digital device. Specifically, the lack of computer security software, virus protection, malicious software, evidence of remote control by another computer system, or other programs or software may assist in identifying the user indirectly and may provide evidence excluding other causes for the presence or absence of the items sought by this application. Additionally, since computer drives may store artifacts from the installation of software that is no longer active, evidence of the historical presence of the kind of software and data described may have special significance in establishing timelines of usage, confirming the identification of certain users, establishing a point of reference for usage and, in some cases, assisting in the identification of certain users. This data can be evidence of a crime, can indicate the identity of the user of the digital device, or can point toward the existence of evidence in other locations. Evidence of the absence of particular data on the drive is not generally capable of being segregated from the rest of the data on the drive.

105. Based upon my training and experience, and information related to me by agents and others involved in the forensic examination of computers and digital devices, I know that, in order to search for data that is capable of being read or interpreted by a computer, law enforcement personnel will need to seize, image, copy, and/or search the following items, subject to the procedures set forth in Attachment C and incorporated by reference herein:

a. Any computer equipment or digital devices that are capable of being used to commit or further the crimes outlined above, or to create, access, or store evidence, contraband, fruits, or instrumentalities of such crimes, as set forth in Attachment B;

b. Any computer equipment or digital devices used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing

equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners that are capable of being used to commit or further the crimes outlined above, or to create, access, process, or store (evidence, contraband, fruits, or instrumentalities) of such crimes, as set forth in Attachment B;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD ROMs, CD Rs, CD RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, personal digital assistants, and cell phones capable of being used to commit or further the crimes outlined above, or to create, access, or store evidence, contraband, fruits, or instrumentalities of such crimes, as set forth in Attachment B;

d. Any documentation, operating logs, and reference manuals regarding the operation of the computer equipment, storage devices, or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles, or similar physical items which are necessary to gain access to the computer equipment, storage devices, or data;

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, storage devices, or data;

h. All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device, that show the actual user(s) of the computers or digital devices during any time period in which the device was used to commit the crimes referenced above, including the web browser's history; temporary Internet files; cookies, bookmarked, or favorite web pages; e-mail addresses used from the computer; MAC IDs and/or Internet Protocol addresses used by the computer; e-mail, instant messages, and other electronic communications; address books; contact lists; records of

social networking and online service usage; and software that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software (or alternatively, the lack of software that may allow others the potential opportunity to control the digital device);

i. All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device, that show evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer or digital device; and all records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device, that show contextual information necessary to understand the evidence, contraband, fruits, or instrumentalities described in this attachment.

CONCLUSION AND REQUEST FOR SEALING

106. Based on the information above, I believe probable cause exists for the authorization of search warrants for **Target Locations #1** and **#2**, and for **Vehicles #1, 2,** and **#3**, and for the issuance of a criminal complaint and arrest warrants for HICKS, JONES, ARREOLA-MARTIN, and POOL, all for Conspiracy to Commit Wire Fraud in violation of 18 U.S.C. § 1349.

107. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation, giving targets an opportunity to destroy or tamper with evidence, change patterns of behavior, notify confederates, and flee from prosecution.

Respectfully Submitted,

ARMANDO DELGADO-CAMPOS
Special Agent, FBI

Subscribed and sworn to me on this 11 day of February 2020.

HON. JOSEPH C. SPERO
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-1

The property to be search is 4865 Mallard Ct., Oakley, CA ("**Target Location #1**") further described as a single story, light-green colored, single-story residence located at the intersection of Mallard Ct. and Lois Ln. (See photograph, below.) **Target Location #1** is on the north side of Mallard Ct. and the front of the residence faces south onto Lois. Ln. The front of **Target Location #1** has four rectangle/squared windows on its facing as well as one circular window above the front door. The address number of "**4865**" is found on the garage to the left of the two-car white-colored garage door. The main entrance to **Target Location #1** is a brown-colored front door down a short cement pathway to the left of the garage.

The areas to be searched shall include all attached rooms, attics, basements, porches, locked containers and safes, and other parts within **Target Location #1**, as well as the surrounding grounds, driveway, garages, campers, carports, storage rooms, storage lockers, yards, trash containers, and outbuildings that are associated with or assigned to **Target Location #1**.

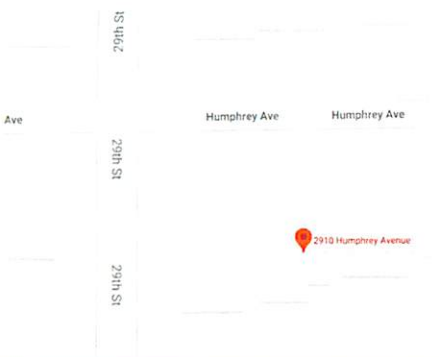
The search shall also include vehicles parked in parking spaces dedicated to **Target Location #1**, vehicles whose keys are present in **Target Location #1**, or vehicles for which there is indicia of ownership, registration, or use found at **Target Location #1.**

Photograph of Target Location #1:

ATTACHMENT A-2

The property to be search is 2910 Humphrey Avenue, Richmond, CA 94804 ("**Target Location #2**") further described as a single story, tan colored house with a garage attached, with a brown roof located almost on the southwest corner of 29th Street and Humphrey Avenue in Richmond, CA. **Target Location #2** front door is white and faces Humphrey Avenue to the North. On the curve directly in front of **Target Location #2** the numbers "2910" are painted with white paint

The areas to be searched shall include all attached rooms, attics, basements, porches, locked containers and safes, and other parts within **Target Location #2**, as well as the surrounding grounds, driveway, garages, campers, carports, storage rooms, storage lockers, yards, trash containers, and outbuildings that are associated with or assigned to **Target Location #2**. The search shall also include vehicles parked in parking spaces dedicated to **Target Location #2**, vehicles whose keys are present in **Target Location #2**, or vehicles for which there is indicia of ownership, registration, or use found at **Target Location #2.**



ATTACHMENT B

Items to be seized

The following items to be seized in whatever form (including electronic) found at the Property to be Searched described in Attachment A-1 ("**Target Location #**1) and Attachment A-2 **(Target Location #2**"), including any digital devices, for evidence, fruits or instrumentalities of violations of 18 U.S.C. § 1343, 18 U.S.C. § 371, 18 U.S.C. § 1028A, and 18 U.S.C. § 1029. These records and materials are more specifically described below.

1. Records, documents, or materials that identify the persons who have possession, custody, or control over the property and vehicles searched, including but not limited to, personal mail, checkbooks, personal identification, notes, other correspondence, utility bills, rent receipts, payment receipts, financial documents, keys, photographs (developed or undeveloped), leases, mortgage bills, vehicle registration information or ownership warranties, receipts for vehicle parts and repairs and telephone answering machine instructions;

2. Any documents, receipts, or records pertaining to the purchase, sale, or transfer of gold or silver coins or bars, or other precious metals. These documents, receipts, and records include, but are not limited to receipts, packaging, boxes, invoices, correspondence, logs, or receipts. Also, any telephone and address books, letters, telephone bills, personal notes, and other items reflecting names, addresses and telephone numbers of individuals who requested or obtained gold coins, gold bars, or other precious metals;

3. Any gold or silver bars, coins, or packaging, and receipts for the purchase of these items;

4. Money ledgers, distribution or customer lists, price lists, supplier lists, maps and written directions to locations, correspondence, notation logs, receipts, journals, books, pay and owe sheets, telephone records, telephone bills, address books, bank statements, storage unit receipts, wire transfer receipts, and other documents or devices noting the price,

quantity, dates, and/or times when gold or silver bars or coins, or other precious metals were purchased possessed, transferred, distributed or sold;

5. The following additional evidence, fruits, and instrumentalities of the above-listed violations of federal law:

   a. Names and contact information of individuals who may be engaged in the purchase of gold or silver coins or bars, or other precious metals with illicit funds;

   b. Logs of calls (which would include last numbers dialed, last calls received, time of calls and duration of calls) both to and from a mobile telephone;

   c. Text messages relating to or referencing the purchase, receipt, sale, or transport of gold or silver bars or coins, or other precious metals;

   d. Incoming and outgoing voice mail messages relating to or referencing the purchase, receipt, sale, or transport of gold or silver bars or coins, or other precious metals;

   e. Browser messages and/or internet communications (e.g., e mail; text messages) relating to the purchase, receipt, sale, or transport of gold or silver bars or coins, or other precious metals;

   f. Documents in electronic format relating to or referencing the purchase, receipt, sale, or transport of gold or silver bars or coins, or other precious metals;

   g. Photographs and videos reflecting the purchase, receipt, sale, or transport of gold or silver bars or coins, or other precious metals.

6. Devices or media that store data electronically, including personal computers, desktop computers, laptop computers, tablet computers, PDAs; iPads; mobile telephones or smartphones, pagers and answering machines (collectively, "Electronic Devices") that could contain evidence of the purchase, receipt, storage or transport of gold and silver

bars and coins, and other precious metals, including the items and materials listed in the paragraphs above.

7. The terms "records," "documents," and "materials" include all of the items described above in whatever form and by whatever means they may have been created and/or stored. This includes any photographic, mechanical, electrical, electronic, and/or magnetic forms. It also includes items in the form of computer hardware, software, documentation, passwords, and/or data security devices, as more fully described below;

8. Computers or storage media used as a means to commit the violations described above, including violations of 18 U.S.C. § § 1343, 18 U.S.C. § 371, 18 U.S.C. § 1028A, and 18 U.S.C. § 1029.

9. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

    b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

    c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER; records of or information about Internet Protocol addresses used by the COMPUTER;

k. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

l. contextual information necessary to understand the evidence described in this attachment;

m. Routers, modems, and network equipment used to connect computers to the Internet.

10. As used above, the terms "records" and "information" includes all forms of creation or

storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

11. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

12. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

ATTACHMENT C

PROTOCOL FOR SEARCHING DEVICES OR MEDIA THAT STORE DATA ELECTRONICALLY

1. In executing this warrant, the government will begin by ascertaining whether all or part of a search of a device or media that stores data electronically ("the device") reasonably can be completed at the location listed in the warrant ("the site") within a reasonable time. If the search reasonably can be completed on site, the government will remove the device from the site only if removal is necessary to preserve evidence, or if the item is contraband, a forfeitable instrumentality of the crime, or the fruit of a crime.

2. If the government determines that a search reasonably cannot be completed on site within a reasonable time period, the government must determine whether all or part of the authorized search can be completed by making a mirror image of, or in some other manner duplicating, the contents of the device and then conducting the forensic review of the mirror image or duplication off site. The government will complete a forensic review of that mirror image within 120 days of the execution of the search warrant.

3. In a circumstance where the government determines that a mirror image of the contents of a device cannot be created on site in a reasonable time, the government may seize and retain that device for 60 days in order to make a mirror image of the contents of the device.

4. When the government removes a device from the searched premises it may also remove any equipment or documents ("related equipment or documents") that reasonably appear to be necessary to create a mirror image of the contents of the device or conduct an off-site forensic review of a device.

5. When the government removes a device or related equipment or documents from the site in order to create a mirror image of the device's contents or to conduct an off-site forensic review of the device, the government must file a return with a magistrate judge that identifies with particularity the removed device or related equipment or documents within 14

calendar days of the execution of the search warrant.

6. Within a reasonable period of time, but not to exceed 60 calendar days after completing the forensic review of the device or image, the government must use reasonable efforts to return, delete, or destroy any data outside the scope of the warrant unless the government is otherwise permitted by law to retain such data.

7. The time periods set forth in this protocol may be extended by court order for good cause.

8. In the forensic review of any device or image under this warrant the government must make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, or other electronically-stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

9. For the purposes of this search protocol, the phrase "to preserve evidence" is meant to encompass reasonable measures to ensure the integrity of information responsive to the warrant and the methods used to locate same.